https://www.wealthmanagement.com/technology/ai-will-heighten-cybersecurity-risks-rias

William Whitehurst/The Image Bank/Getty Images

TECHNOLOGY

AI Will Heighten Cybersecurity Risks for RIAs

While scams like email impersonation and phishing are nothing new, generative AI has supercharged the risks by introducing new threats, including deepfakes and malicious chatbots.

Rob Burgess | Jul 12, 2023

Imagine receiving a phone call from someone you believe to be one of your clients. They are asking you to move some money around for them. It sounds like the client. And the voice on the other end is able to answer your simple questions quickly, clearly and accurately. But, before completing the transaction, there's one small detail you should probably know: The voice is artificial and run by scammer who has scraped the unsuspecting client's voice and personal details for their own purposes.

This sort of scenario is exactly what Lee W. McKnight, associate professor in the School of Information Studies at Syracuse University, said he sees becoming commonplace, especially in the wealth management industry, as fraud and scams are amplified and enhanced with technological advances coming from increasingly available artificial intelligence applications.

“Everybody wants to talk about making money of course in the sector, but nobody wants to think about the risks,” said McKnight. “This is like alarm-level concern I would have as keepers of high-value data on high-value targets.”

Cybersecurity threats aren’t new. A survey released last month by BlackFog using Sapio Research gathered responses from 400 IT decision-makers in the U.S. and U.K. from companies with 100 to 999 employees and found 61% of these small- and medium-sized businesses had experienced a cyberattack in the last year. Of those, 87% experienced two or more successful cyberattacks.

But what is new is how the advent of widespread generative artificial intelligence has dramatically shifted what’s possible for professional cybercriminal groups and hostile nation-states seeking to fleece advisors and their clients.

“It doesn’t feel like the sector has really woken up to just how much the world has changed with AI,” McKnight said. “There’s a shift in the maturity of the technology and the range of applications, which makes it way easier to do funkier things to RIAs and their clients that cause them to lose a lot of money.”

AI Uses Public Data to Fine-Tune Phishing Attacks

In a January 2020 episode of the podcast “Transparency with Diana B.,” Diana Britton, managing editor of WealthManagement.com, was joined by Darrell Kay, principal of Kay Investments, who related the story of how, in the summer of 2018, he received an email from an affluent client asking him to move $100,000 to a different bank than usual. What Kay didn’t know was that he was communicating with a scammer who had hacked into the client’s email. Luckily, the bank stepped in and returned the client’s money.

These kinds of phishing scams could be supercharged by the way AI can give malevolent actors greater scale. “It suddenly becomes very cheap to imitate thousands of scammers at once, just keep running ChatGPT instead of the scammer having to interact with each mark as a person,” said Dr. Shomir Wilson, assistant professor in the College of Information Sciences and Technology at Penn State University.

The ability of generative AI to raise the quality and quantity of email attacks has even McKnight, who studies cybersecurity for a living, performing double takes. For example, he said he received an email from a former doctoral student from a decade prior asking him for $200 by the end of the month.

“It looked like his email,” said McKnight. “Everything looked legit.”

After closer inspection, though, McKnight concluded someone had hacked into his former student’s email and sent a series of ChatGPT-generated automated messages to everyone in their address book. McKnight said these sorts of targeted attacks are usually easily detectable due to inherently poor spelling and unnatural grammar. Not so, this time.

“It was all perfect. It was all done properly,” said McKnight. “If it’s the contact list of … investment advisory firms it’s not going to be $200 they’re asking for, right? But it’s similar.”

Jim Attaway, chief information security officer at AssetMark, said in the past, phishing attacks targeting RIAs often contained obvious indicators that made them easier to spot and classify as fraudulent. Today, AI has changed the game, creating perfectly targeted messages. When AI is combined with access to an individual’s or company’s social media channels, scammers can pull information from messages that reference recent events or individual connections, making attacks highly targeted and accurate.

McKnight said this sort of attack was particularly dangerous for advisors, whose business is largely based on personal interactions.

“Your client told you they want to do something urgently, your first thing is to think about doing it and not quite checking as much as you might,” said McKnight.

Once hackers gain access to a system through impersonation or credential theft, malware can monitor an RIA or client’s activity and potentially allows the bad actor to operate from within either environment, according to Attaway.

Generative AI also has the potential to increase the sophistication of cybersecurity attacks and compromise networks by helping scammers ingest as much information as possible about a target for purposes of manipulation or social engineering, added Steven Ryder, chief strategy officer at Visory.

Traditionally, cyberattacks have been broad and generic, but as AI technology advances, attackers are increasingly leveraging information across social media channels and public records to create targeted attacks on RIAs that successfully impersonate clients by gaining trust and exploiting vulnerabilities, Attaway said.

Wally Okby, strategic advisor for wealth management for Datos Insights (formerly the Aite-Novarica Group), said the information needed to conduct a convincing social engineering scam on a selected mark is more readily available to cybercriminals.

“Communication is being monitored everywhere now and one would be naïve to think otherwise,” said Okby. “You can be sure there are people and parties behind the scenes that could potentially weaponize that communication.”

Coming Soon to a Scam Near You: Deepfakes

One new and devious method generative AI lends itself to is audio, visual and video impersonation, also known as a deepfake.

“It’s now much easier to do that,” said McKnight. “It’s not Hollywood CGI quality but that’s something that’s real that’s happened, and companies have lost significant funds that way.”

Attaway said while these sorts of attacks are currently less common, deepfake technology is continuing to evolve, potentially enabling cybercriminals to use AI to manipulate audio and video clips that can be used to impersonate clients. RIAs may experience attacks that recreate clients’ voices, sometimes with real-time responses, leading to more convincing and deceptive attacks.

In fact, market research company MSI-ACI released the results of a recent survey of 7,000 adults from nine countries and found one in four said that they had experienced an AI voice cloning scam or knew someone who had. Of those surveyed, 70% said they weren’t confident they could tell the difference between a cloned voice and the real thing.

In a deepfake scam, an advisor could receive an urgent voicemail from someone they believe to be a client speaking in what sounds like their voice, said McKnight. An advisor may even call back to confirm it’s real, but generative AI has the potential to keep the conversation going convincingly in a back-and-forth setting.

Video is a further check over audio, but even that has the potential to be deepfaked as the technology evolves. It’s currently difficult today since creating convincing deepfake video requires massive computing power, but that all could change and that “will present tremendous problems” according to Daniel Satchkov, co-founder and president of RiXtrema.

“Video is proof that something happened,” Satchkov said. “And if you think about what happens when video becomes realistically deepfaked, then anything is possible…. Because they will be able to impersonate your colleague or your boss and ask for your password.”

Threats from Chatbots Themselves

Aside from scams potentially run by AI technology, another risk presented by generative AI could come from advisors using them for work but inputting sensitive information that could end up being leaked. One way to minimize risk is to never to input sensitive client data into chatbots like ChatGPT, said William Trout, director of wealth management for Javelin Strategy and Research.

Visory's Ryder agreed advisors should think twice about inputting any confidential information about themselves or others into a shared public database that can be accessed by anyone. For example, Ryder said they wouldn’t be sharing their birthday or personal information about themselves or family members with a generative AI app.

Even with generative AI in its nascent stages, leaks of potentially sensitive data have already occurred. In March, OpenAI confirmed a glitch briefly caused ChatGPT to leak the conversation histories of random users.

Leaks aside, Trout said it was clear the iterative nature of machine learning technology meant any information provided will be used to inform the model and recommendations.

Financial advisor Brandon Gibson proactively calls clients directly to confirm sensitive requests.

“The fact that the machine learning engine is using this data to educate itself to me puts this privileged information at risk,” said Trout. “So, don’t put client information into the darn engine. As researchers … we would never put any specific information in there. You don’t ultimately know where it’s going to go.”

In addition to cybersecurity concerns, Trout said this information can be subpoenaed or otherwise accessed by external bodies including regulators.

“It’s less about direct seepage of information and more about kind of letting your privileged client information be used as an input for an output you really can’t visualize,” said Trout. “You can’t assume that anything that goes in there is fully protected. Advisors need to use it as a learning tool but not as a silver bullet for solving client-specific challenges.”

Proposed SEC Cybersecurity Rules on the Way

With AI supercharging these persistent online threats, increased federal oversight and requirements relating to cybersecurity are soon to come.

The Securities and Exchange Commission proposed a new rule on cybersecurity in February 2022 which would pertain to RIAs, as well as registered investment companies and business development companies. If finalized, the rule would require advisors and funds to create reasonably designed policies and procedures to protect clients’ information if a breach occurred and to disclose cyber incidents on amendments to their Form ADVs. Additionally, firms would be tasked with reporting “significant” cyber incidents to the SEC within 48 hours of uncovering the severity of the breach.

In March, SEC commissioners also approved several cyber and data privacy-related rules and amendments, including amendments to Regulation S-P that would require RIAs to “provide notice to individuals affected by certain types of data breaches” that might leave them vulnerable to identity theft.

Additionally, the commission approved a proposed rule updating cybersecurity requirements for broker/dealers, as well as other so-called “market entities,” including clearing agencies, major security-based swap participants and transfer agents, among others. Under the new rule, b/ds must review their cyber policies and procedures so they're reasonably designed to offset cyber risks, akin to the proposal about advisors from last year.

Unlike the advisors' rule, however, b/ds would have to give the SEC “immediate written electronic notice” when faced with a significant cybersecurity incident, according to a fact sheet released with the rule.

Earlier this month, the timeline to finalize the proposed rule was delayed until October.

What Else Can and Should Be Done?

Experts agree that there are many steps advisors can take to reduce their exposure to AI-powered online scams. Chief among them is a strong defensive, privacy-minded posture.

Kamal Jafarnia, co-founder and general counsel at Opto Investments, said cyberattacks assisted by generative AI were of particular concern to the wealth management industry because many independent RIAs are small firms with limited budgets.

Attaway said many RIAs traditionally manage their IT infrastructure internally or rely on third-party providers for technical support. These limit advisors’ ability combat threats effectively. Unlike larger corporations with dedicated IT security teams and budgets, RIAs often lack access to sophisticated security software that can help mitigate risk or don’t know where to look to find free or inexpensive solutions to provide some of the same protections.

In March 2023, the T3/Inside Information Advisor Software Survey, which collected 3,309 responses, revealed that cybersecurity software is being used by just 24.33% of respondents, up less than two percentage points from the previous year's survey. Despite this, among those who use cybersecurity software, respondents reported an average of 8.25 on a satisfaction scale of 1 to 10—the highest satisfaction rate of any technology category.

From a network or operations perspective, Ryder said generative AI itself can be very useful in monitoring potential cybersecurity breaches by searching for patterns in behaviors and activities. For example, Ryder said they were using AI to determine normal versus unusual activity, which can help them prevent, isolate and stop cybersecurity incidents.

Visory Chief Strategy Officer Steven Ryder warns advisors against inputting sensitive client data into chatbots like ChatGPT.

Data protection should be at the top of the priority list for every RIA, said Scott Lamont, director of consulting services at F2 Strategy. There should be a focus on client education on avoiding phishing threats, being secure where and when accessing data and leveraging technologies to protect and manage credentials. That same education should be shared with advisors and operations and support staff, because of the considerable volume of personally identifiable information they access.

Firms can seek out technology partners that use AI-enabled tools in their cybersecurity stack and are taking the right steps to safeguard themselves against sophisticated attacks, said Ryder.

Since most RIAs are leveraging third-party tools, Lamont said it's critical to stay on top of the vendors' policies on data protection.

Attaway said RIAs must stay aware of client contact information and actively look for obvious signs of impersonation, such as incorrect email addresses or harmful links. However, RIAs should reinforce their defenses with additional layers of technological protection. The most important method of protection is the implementation of password managers such as LastPass or 1Password and multi-factor authentication on all applications.

The widespread adoption of MFA as a defensive measure has grown considerably in recent years. The 2023 Thales Global Data Threat Report survey, conducted by S&P Global Market Intelligence with nearly 3,000 respondents across 18 countries, found that while MFA adoption was stagnant at 55% for 2021 and 2022, in 2023, it jumped to 65%.

Using such protection across email and company accounts is imperative to improving security as a foundational barrier of protection, said Attaway. An advisor’s email is typically the key to their world. With control of it, passwords can typically be reset and communications from it are generally considered authentic. MFA can make this virtually impossible for an attacker when coupled with a tool such as Microsoft or Google Authenticator, both of which are free to use.

Attaway further recommended upgrading to Office365 E5, which allows users to block malicious messages and includes integrated security capabilities that provide an additional layer of protection through reputational monitoring. Firms can also use OpenDNS, a free service for personal use and a low-cost option for businesses, which blocks material based on reputation as well as content. RIAs must also ensure machines are patched, and that the Windows firewall and scanners are active, said Attaway. This will help to prevent direct attacks from a bad actor on the RIA's equipment.

Additionally, McKnight recommended every advisor purchase personal cyber insurance.

Brandon Gibson, a 46-year-old advisor with Gibson Wealth Management in Dallas, said MFA is helpful in screening for threats, as is proactively calling clients directly to confirm sensitive requests.

“My clients trust me to keep their information safe,” said Gibson. “I can’t provide the services I do without that trust.”